Embassy of the United States of America

American Citizen Services
24 Grosvenor Square
London, W1A 2LQ

ATM FRAUD IN THE UNITED KINGDOM

ATMs have become one of the most convenient and efficient ways for travelers in the United Kingdom to obtain local currency. Most machines accept American bank cards and will give you pounds while deducting dollars from your U.S. account, usually at a more favorable exchange rate than you would get for cash or traveler's checks. However, use of these machines is not without risk. ATM fraud in the United Kingdom has increased significantly over the past few years and is becoming more sophisticated, incorporating technologies to record surreptitiously customer ATM card and PIN information. In order to avoid being victimized, visitors should be aware of the types of ATM scam that can occur.

A normal ATM device.

ATM with skimming device attached in front of card slot. Notice how the card slot is no longer inset into the machine, but "bulges" outward.

ATM fraud in the United Kingdom generally comes in three varieties: card-reading devices, card-trapping devices, and distraction schemes.

1. Card Reading Devices. Criminals alter the ATM itself by adding a skimming machine and a mini-camera to it. The first device, mounted on the card entry slot, reads the bar code on your card. The second records you as you enter your PIN. After you complete your transaction, receive your card, and walk away, someone else has your number and your access code. Usually, the perpetrators make a new card and use it to withdraw money from your account. The skimming devices are

not always easy to spot, especially if you are unfamiliar with the look of UK ATMs.

2. Card-Trapping Devices. An alternative form of altering the ATM itself involves inserting a thin ribbon of x-ray tape into the card slot. The loop traps your card and makes it seem as though the bank has repossessed it. At this point, someone else, a purported "Good Samaritan," comes along and tells you that you can retrieve your card by re-entering your PIN code. He watches while you do so. After your card still refuses to emerge and you walk away from the ATM, the perpetrator removes the device and your card, which he then uses to withdraw money from your account.
3. Distraction Schemes. Distraction schemes do not rely on tampering with ATM machines themselves; instead, they involve interrupting you while you are withdrawing funds. Typically, there are two perpetrators, one who distracts you after you have entered your card and PIN, and another who grabs your money. The distractor may pretend to sell or give you a newspaper; place a £5 note at your feet and tell you that you dropped some money; ask you for a charitable donation; or whisper in your ear. Sometimes the distractors are children. The common element in all these ruses is that they occur after you have entered your card and your PIN and are no longer protected by the bank's security features.

In order to prevent becoming the victim of such scams:

- If possible, use ATMs located inside buildings or in bustling public places where it is difficult for criminals to tamper with the machines. Do not use machines in isolated areas or at night.
- Avoid ATMs where the card slots appear to have been mounted on the machine (see illustration). Card entry slots should be flush with the surface of the ATM or recessed from it. If you see a card entry slot that is raised above the machine, it should raise your suspicions and you should not use it.
- If you find it awkward to read the screen or enter your PIN, do not use the machine. It may have been altered. Legitimate displays are never mounted in front of ATMs. Anything that blocks or partially obscures a sign may house a camera.
- Guard your PIN, especially when entering it, by shielding the keypad with one of your hands.
- If possible, have a friend or partner accompany you while you make a withdrawal.
- If you are distracted at all during an ATM transaction, immediately press cancel and collect your card before responding to anyone who has accosted you.
- If a machine swallows your card, call the bank's toll-free number (usually posted on or near the ATM) and report it.

- Change your PIN from the original number given when you first got your card (this number is sometimes contained in the data on the magnetic strip and can be discovered by thieves who have stolen your card). Do not keep your account number and PIN together.

If in spite of such precautions you do find yourself the victim of ATM fraud, do the following:

- If you discover a card reader or card-trapping device, do not remove it. The criminals may be watching the location and will want to recover their equipment. Instead, call the police at 999.
- Call your bank to alert it that you have lost your card and to refuse all new withdrawals. This will be easier if you carry the bank's phone number with you on your trip.
- If someone whose behavior raises your suspicion approaches you at an ATM, do not challenge the person but keep track of the details and report the matter to the police as soon as possible.
- If you discover the fraud after you return to the United States, you can (and should) still file a police report in the United Kingdom. To do so, go to http://www.met.police.uk/reporting_crime/index.htm#online.

If you are in the United Kingdom, you also may call the U.S. Embassy in London at 020-7499-9000, or email us at SCSLondon@state.gov. Within the United States, you may call the Department of State's Office of Overseas Citizens Services at toll-free at 1-888-407-4747.